

APPROVED	PPROVED O.G. FIG.		
BY	CLASS	SUBCLASS	
DRAFTSMAN			

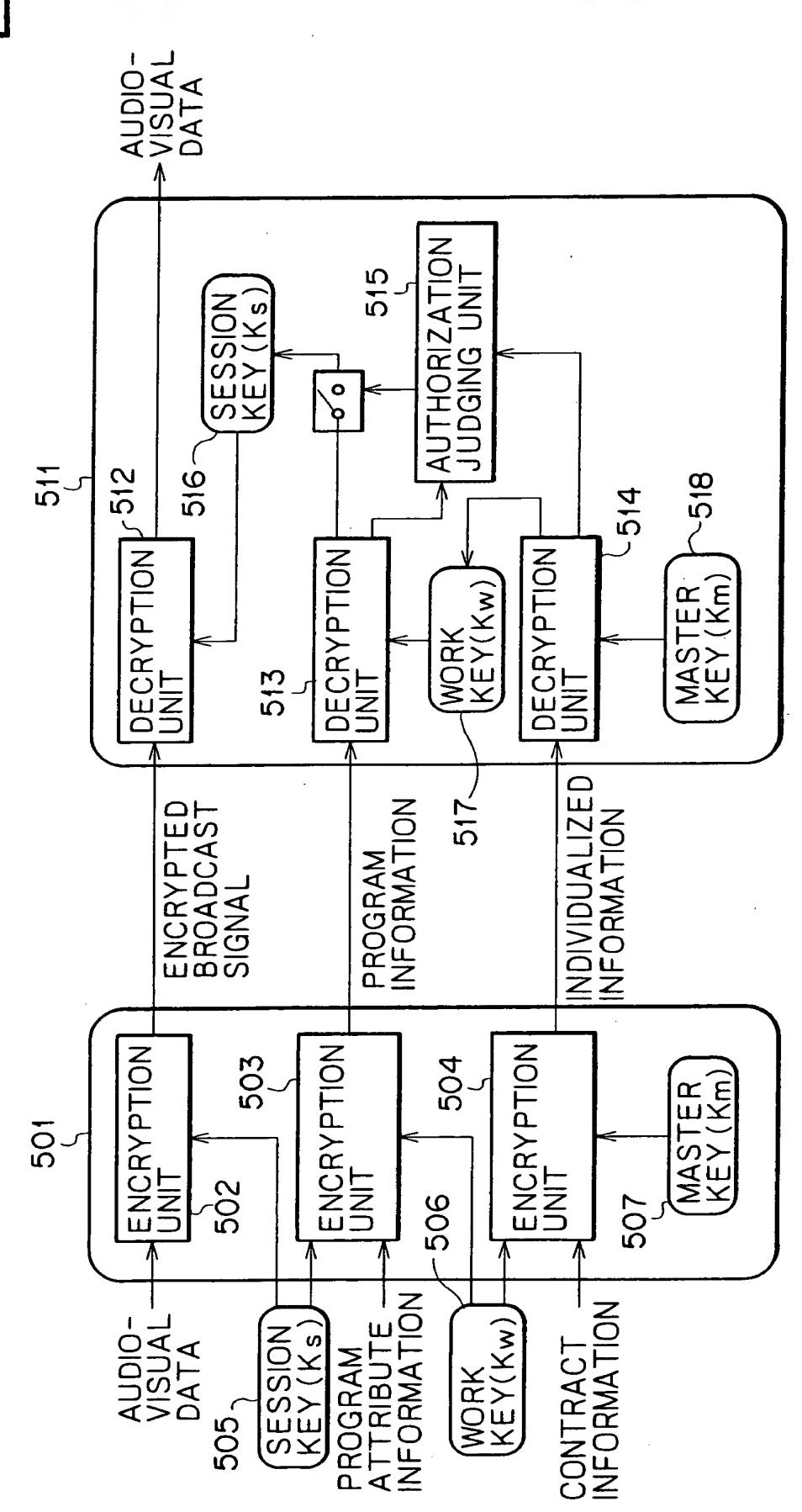
F | G 4

		_
413 در	ADAPTATION PAYLOAD FIELD (INFORMATION)	
	ADAPTAT I ON F I ELD	8×Nbits
	CYCL IC COUNTER	4bits
	ADAPTAT 10N F 1 ELD CONTROL	2bits
412 \	SCRAMBLE CONTROL	2bits
411	PID	13bits
	TRANSPORT PACKET PRIORITY	1bit
	UNIT START INDICATION	1bit
	ERROR INDICATION	1bit
	SYNCHRO- NIZING BYTE	8bits

188bytes

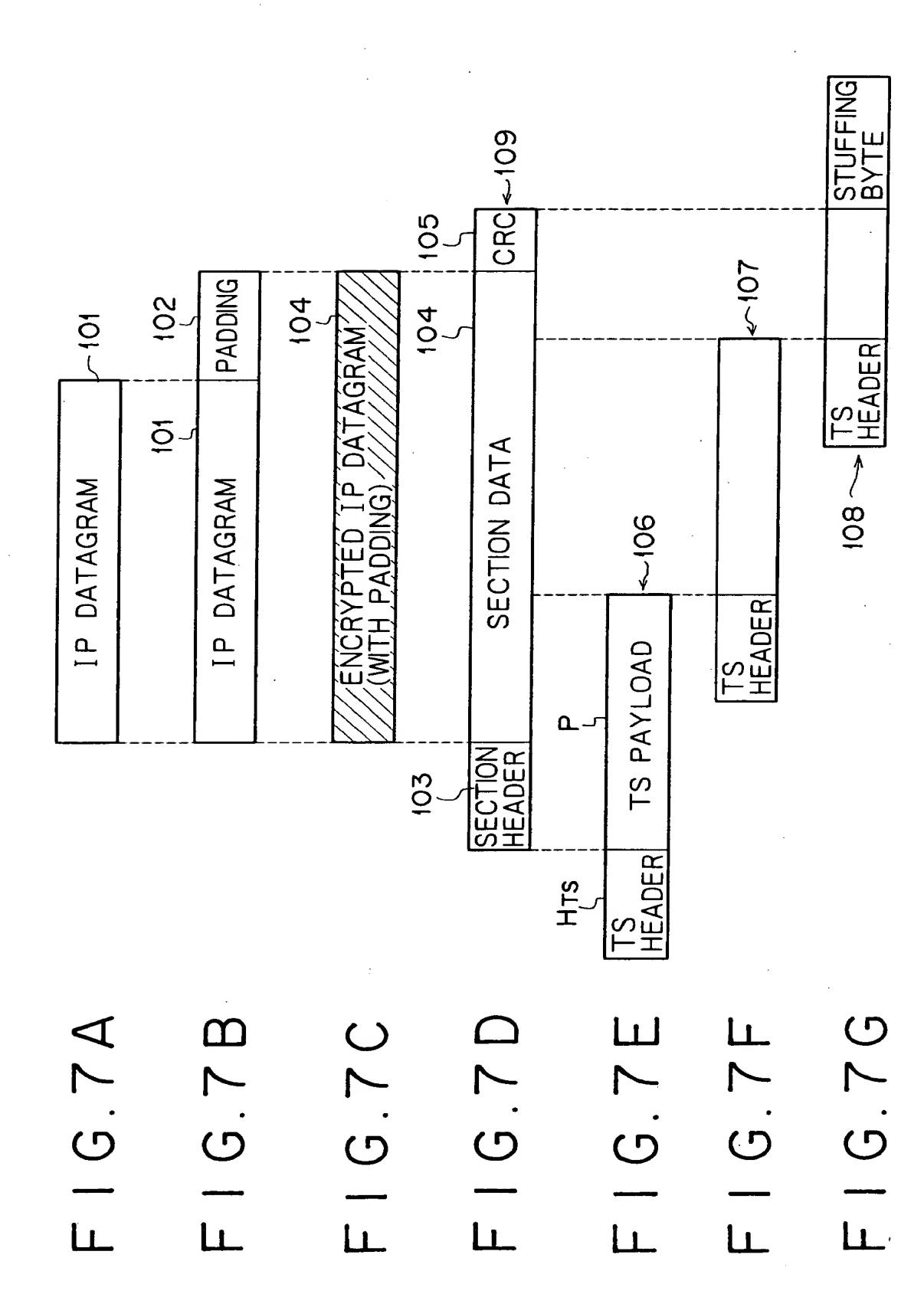
APPROVED O.G. FIG.
BY CLASS SUBCLASS
ORAFTSMAN

下 (5)



APPROVED	O.G. FIG.		
BY	CLASS	SUBCLASS	
DRAFTSMAN			

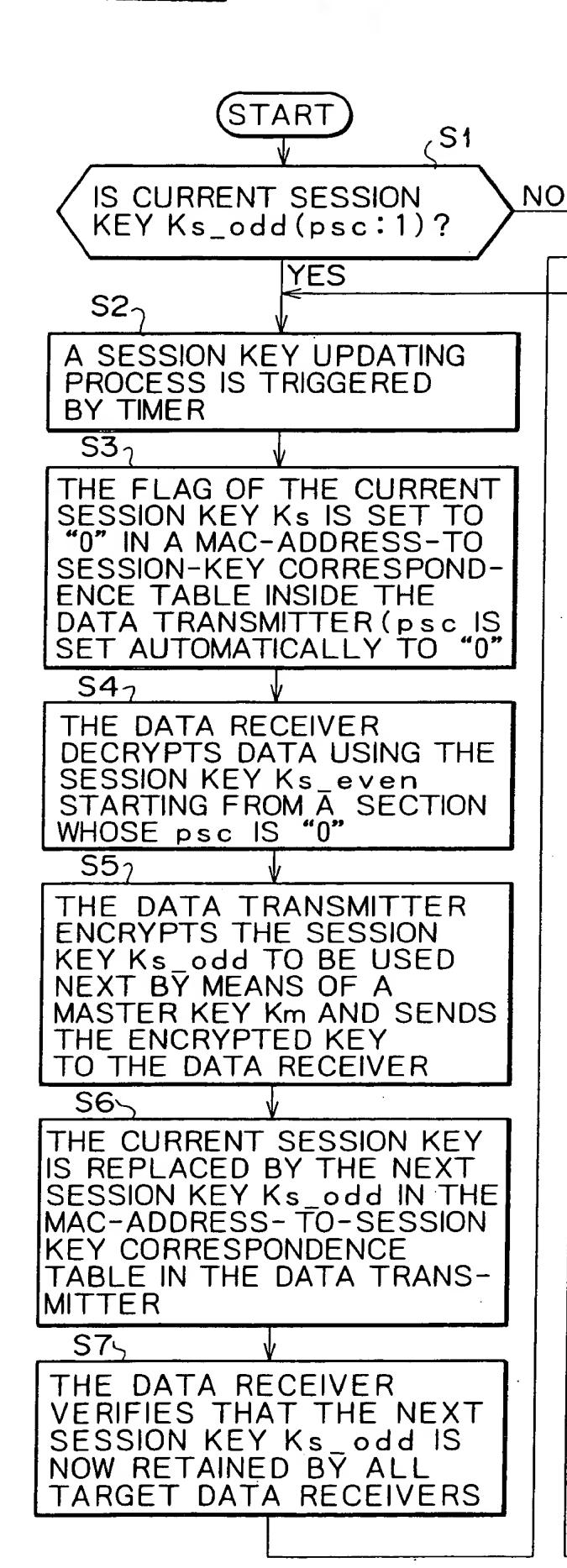
30 53b 53c DATA RECEIVER DATA RECEIVER DATA RECEIVER 40 ~ **@** ò Ŋ INTERNET SERVICE PROVIDER DATA TRANSMITTER INTERNET **%**



APPROVED	O.G. FIG.		
ВУ	CLASS SUBCLASS		
DRAFTSMAN			

131 32 34 CA MANAGING UNIT DECRYPTION DECRYPTION UNIT (33 MASTER KEY (Km) SESSION KEY (Ks) N 35 RESTRICTIVE DATA TRANSMISSION CONTROL INFORMATION ENCRYPTED SESSION KEY Ks ENCRYPTED DATA CA MANAGING UNIT ENCRYPTION ENCRYPTION UNIT 22 25 √<u>7</u> (23 MASTER KEY (Km) 7-۲ DATA -SESSION KEY (Ks) 24

/ PPROVED	O.G. FIG.	
BY	CLASS	SUBCLASS
DF FTSMAN		



F I G.9

A SESSION KEY UPDATING PROCESS IS TRIGGERED BY TIMER

S8

ς **S9**

< S10

ς S11

cS12

< S13

THE FLAG OF THE CURRENT SESSION KEY Ks IS SET TO "1" IN A MAC-ADDRESS-TO SESSION-KEY CORRESPOND-ENCE TABLE INSIDE THE DATA TRANSMITTER (psc IS SET AUTOMATICALLY TO "1"

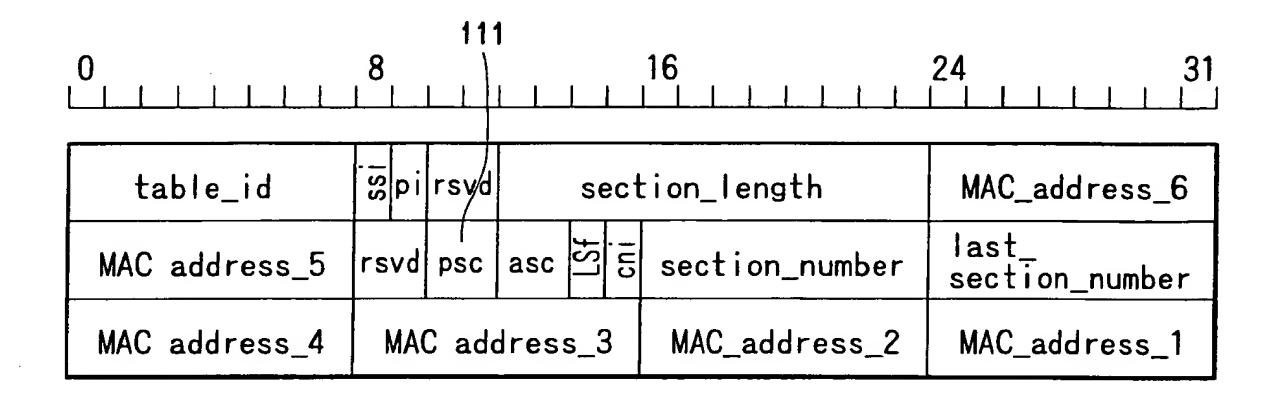
THE DATA RECEIVER
DECRYPTS DATA USING THE
SESSION KEY Ks_odd
STARTING FROM A SECTION
WHOSE psc IS "1"

THE DATA TRANSMITTER ENCRYPTS THE SESSION KEY Ks_even TO BE USED NEXT BY MEANS OF THE MASTER KEY Km AND SENDS THE ENCRYPTED KEY TO THE DATA RECEIVER

THE CURRENT SESSION KEY IS REPLACED BY THE NEXT SESSION KEY Ks_even IN THE MAC-ADDRESS-TO-SESSION KEY CORRESPONDENCE TABLE IN THE DATA TRANS-MITTER

THE DATA RECEIVER
VERIFIES THAT THE NEXT
SESSION KEY Ks_even IS
NOW RETAINED BY ALL
TARGET DATA RECEIVERS

F I G.10



section_syntax_indicator private_indicator ssi

рi

rsvd: reserved

payload_scramble_indicator address_scramble_indicator LLC_SNAP_flag current_next_indicator psc asc

LSf

cni ·

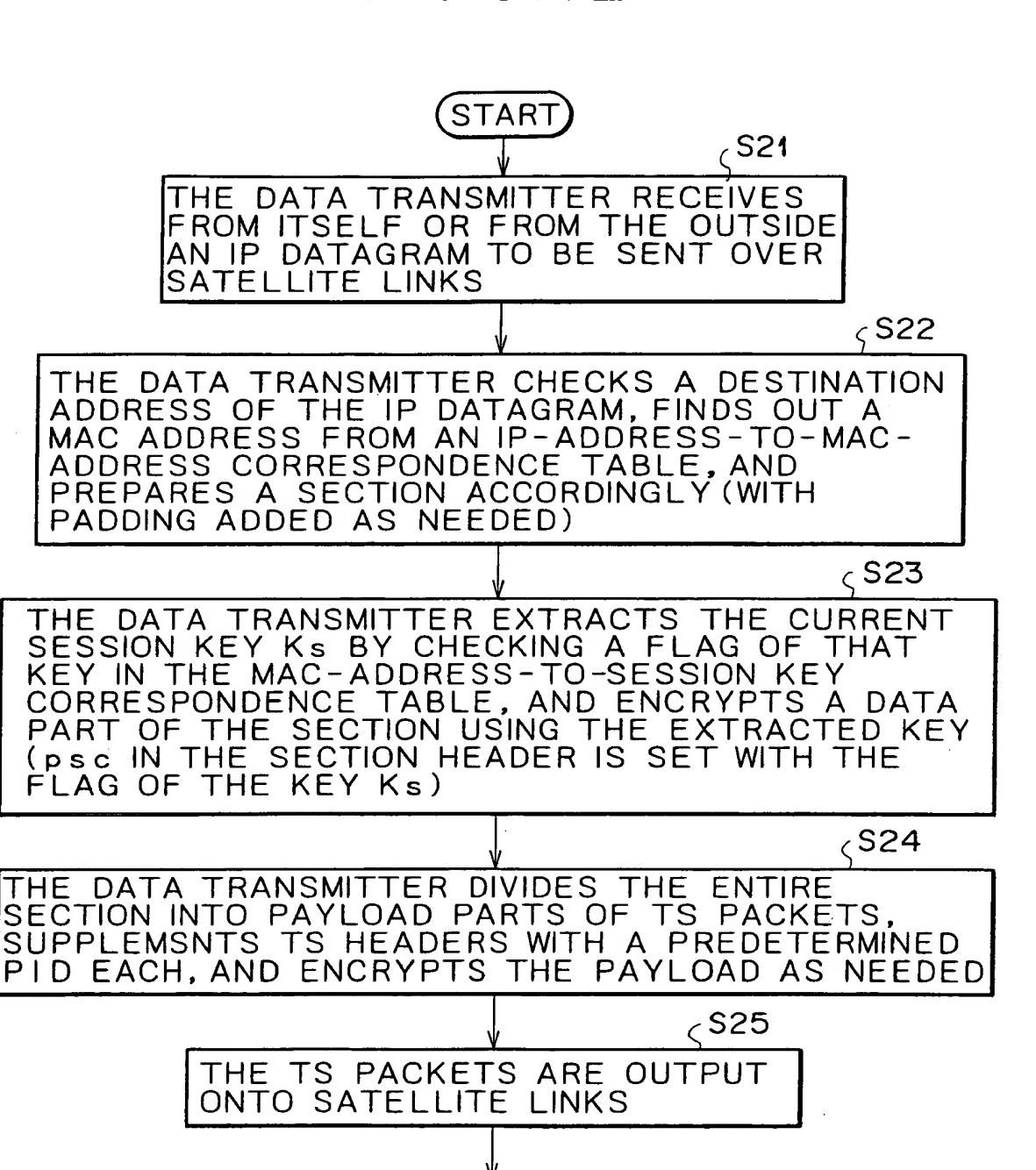
F I G.11

112

MAC ADDRESS	Ks_even	Ks_odd	Ks FLAG
08:00:46:01:07:24	0×C08F25	0×90B3AF	0
08:00:45:01:07:09	0×26D261	0×BA023C	1
01:00:5e:16:0:0	0×461E67	0×DC1A22	0

APTROVED O.G. FIG.
BY CLASS SUBCLASS
DRAFTSMAN

F I G.12



END

APPROVED O.G. FIG.
BY CLASS SUBCLASS
ORAFTSMAN

F I G.13

IP ADDRESS	bitmask	MAC address
133. 11. 9. 39	255. 255. 255. 225	08:00:46:01:07:24
133. 11. 20. 0	255. 255. 255. 0	08:00:46:01:07:09
226. 0. 0. 0	255. 255. 254	01:00:5e:16:0:0

F I G.15

MAC ADDRESS	Ks_even	Ks_odd
08:00:46:01:07:24	0×C08F25	0×90B3AF
01:00:5e:16:0:0	0×461E67	0×DC1A22

F I G.16

113

VERS	HLEN	SERVIE TYPE	T	OTAL LENGTH
	IDENTIFICAION		FLAGS	FRAGMENT OFFSET
TIME TO LIVE PROTOCOL		PROTOCOL	H	EADER CHECKSUM
		SOURCE IF	ADDRE	ESS ·
	DESTINATION IP ADDRESS			
	IP OPTIONS (IF AI		1Y)	PADDING
	DATA			
				·

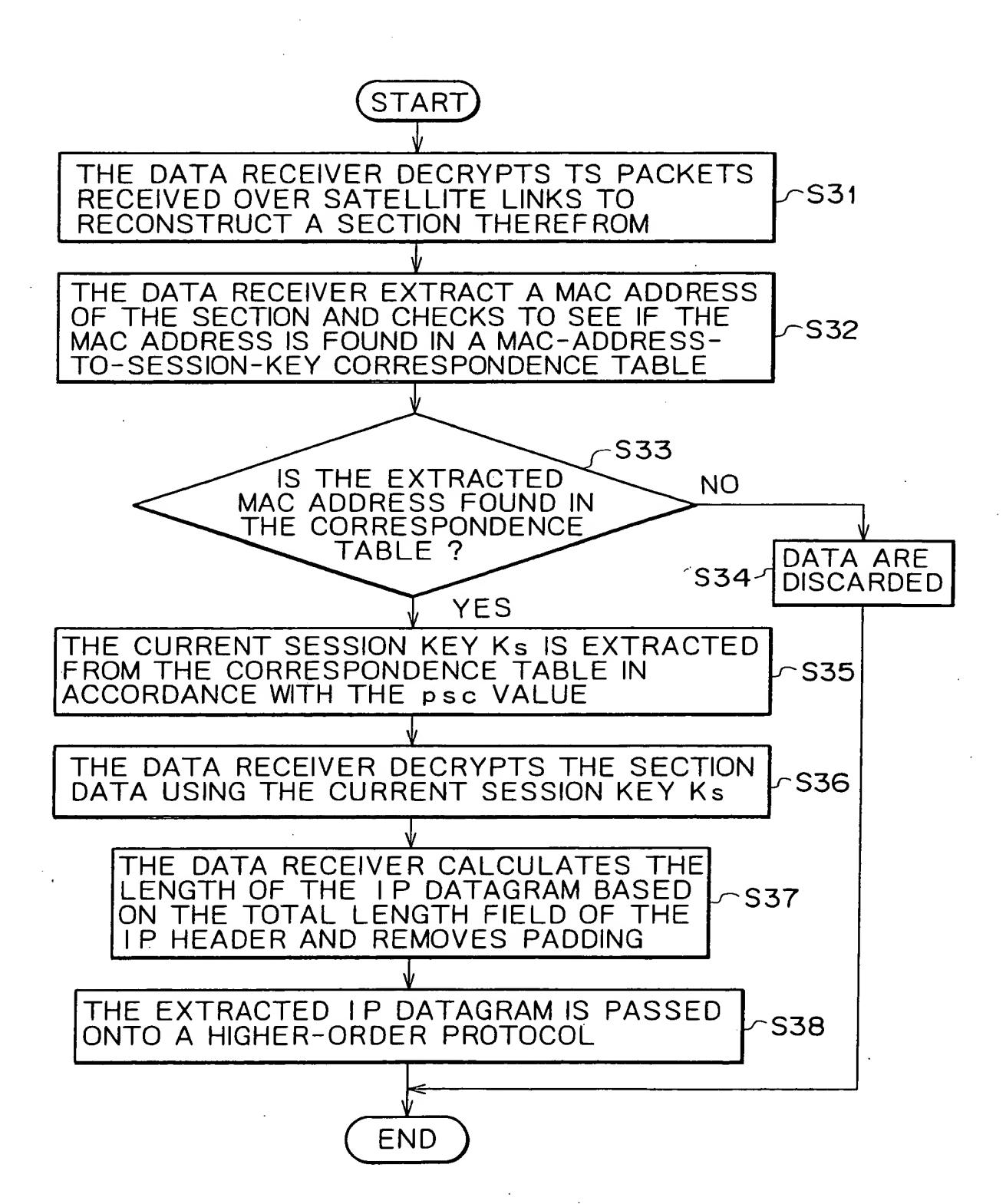
APPROVED

O.G. FIG.

S SUBCLASS

F I G.14





APPROVED	O.G. FIG.		
BY	CLASS	SUBCLASS	
DRAFTSMAN			

F 1 G.17

COMPUTER 202 DATA RECEIVER (ROUTER) LOCAL AREA NETWORK **3**d COMPUTER 40 203a DATA TRANSMITTER

O.G. FIG.

SUBCLASS

